REMARKS

Applicant's representative appreciates the courtesies extended during the telephonic interview of November 10, 2009. The amendments and remarks made herein are in accordance with those discussed during the telephonic interview.

The Non-Final Office Action mailed September 16, 2009 considered and rejected claims 1-20. Claims 1-20 were rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. Claims 1-20 were rejected under 35 U.S.C. 103(a) as being unpatentable over White et al. ("Anatomy of a Commercial-Grade Immune System") hereinafter *White* in view of Schultz et al. (US 2003/0065926) hereinafter *Schultz* in further vie of Applicant Admitted Prior Art referred to hereinafter by AAPA.[1]

A. Response to Objections to Specification

With respect to the trademarks mentioned in the Specification, Applicant has amended the Specification as requested. In addition, Applicant has amended the Specification to address the informalities noted on pages 2-3 of the Office Action.

Applicant has also amended the Specification to clarify computer-readable media and, in particular, distinguish computer-readable storage media (*e.g.*, RAM, ROM, EEPROM, CD-ROM) from computer-readable transmission media (*e.g.*, carrier waves). No new matter has been added via this amendment. The amendment above notes that computer storage media and transmission media are "two distinctly different kinds of computer-readable media." Applicant has amended claims 4, 14-16 and 20 to limit them to computer-readable storage media. Thus, these claims recite statutory subject matter under 35 U.S.C. 101.

B. Response to Rejection under 35 U.S.C. 112, First Paragraph

The Office Action stated that claims 1-20 failed to comply with the written description requirement based on the following claim language from claims 1-4:

- "wherein a plurality of different execution behaviors of the code module are recorded" and

[1] Although the prior art status of the cited art is not being challenged at this time, Applicant reserves the right to challenge the prior art status of the cited art at any appropriate time, should it arise. Accordingly, any arguments and amendments made herein should not be construed as acquiescing to any prior art status of the cited art.

- "to determine whether the plurality of different execution behaviors recorded in the behavior signature of the code module match a plurality of different execution behaviors recorded in a behavior signature of a known malware" and "the code module is a known malware based at least in part on the degree that the plurality of different execution behaviors recorded in the behavior signature of the code module match a plurality of different execution behaviors recorded in a behavior signature of the known malware."

Applicant traverses this rejection because the present application does provide written description support for claims 1-20.

In further detail, the present application discloses a dynamic behavior evaluation module 204 in which a code module 212 is executed:

> Each dynamic behavior evaluation module, such as dynamic behavior evaluation module 204, represents a virtual environment, sometimes called a sandbox, in which the code module 212 may be "executed." To the code module 212, the dynamic behavior evaluation module 204 appears as a complete, functional computer system in which the code module may be executed. By using a virtual environment in which the code module 212 may operate, the code module may be executed such that its dynamic behaviors may be evaluated and recorded, while at the same time any destructive behaviors exhibited by the code module are confined to the virtual environment.[2]

The present application discloses that, as the code module 212 is executed, the dynamic behavior evaluation module 204 records the execution behaviors of the code module:

> As the code module 212 executes within the dynamic behavior evaluation module 204, the dynamic behavior evaluation module records "interesting" behaviors exhibited by the code module. Interesting behaviors are those which a user or implementer of the malware detection system 200 has identified as interesting, potentially associated with malware, and are used to compare the behaviors of the code module 212 against known malware behaviors.[3]

The present application further discloses a plurality of different execution behaviors that may be recorded in Table A,[4] which is shown below:

[2] *See* U.S. Patent Application Publication 2005/0188272 A1, [0023] (the present application) (emphasis added).
[3] *See* U.S. Patent Application Publication 2005/0188272 A1, [0024] (the present application) (emphasis added).
[4] *See* U.S. Patent Application Publication 2005/0188272 A1, [0024] ("Table A includes an exemplary, representative list of 'interesting' behaviors, including parameters that are also considered interesting, that are recorded by a dynamic behavior evaluation module 204.").

TABLE A

RegisterServiceProcess ( )	ExitProcess ( )
Sleep ( )	GetCommandLine ( )
WinExec (application_name)	CreateProcessA (proces_name, parameters_list)
InternetOpenUrlA (URL_name)	GlobalAlloc ( )
InternetOpenA (URL_name)	GetTickCount ( )
IntenetClosetHandle ( )	CopyFileA (new_name, existing_name)
CreateFileA (file_name)	GetWindowsDirectoryA( )
ReadFile ( )	GetSystemDirectoryA ( )
WriteFile ( )	GetModuleFileNameA ( )
Close Handle ( )	LoadLibraryA (library_name)
RegOpenKeyA (key_name)	GetProcAddress (procedure_name)
RegSetValueA (subkey_name)	FindFirstFileA (file_specificator)
RegSetValuExA (subkey_name)	FindNextFileA ( )
RegCloseKey ( )	FindClose ( )
UrlDownloadToFileA (url_name, file_name)	

The present application further discloses that the term "behavior signature" refers to these recorded execution behaviors: "The dynamic behavior evaluation module 204 records the "interesting" behaviors exhibited by the executing code module 212 in a file, referred to as a behavior signature 210."[5]

The present application discloses that the behavior signature of the code module 212 is compared to the behavior signatures of known malware:

> At block 310, the behavior signature 210 is compared against known malware behavior signatures stored in the malware behavior signature store 208.[6]

Finally, the present application discloses that the system may report whether the code module is a known malware based at least in part on the degree that the execution behaviors recorded in the behavior signature of the code module match the execution behaviors recorded in the behavior signature of the known malware:

> If there was not a complete match between the behavior signature 212 and the behavior signatures in the malware behavior signature store 208, at decision block 318, a further determination is made as to whether there was at least a partial match. If there was a partial match between the behavior signature 210 and a behavior signature in the malware behavior signature store 208, at block 320, the

[5] *See* U.S. Patent Application Publication 2005/0188272 A1, [0024] (the present application) (emphasis added).
[6] *See* U.S. Patent Application Publication 2005/0188272 A1, [0033] (the present application) (emphasis added).

malware detection system reports that the evaluated code module 212 may be malware. As previously discussed, the decision to report that the evaluated code module 212 may be malware may be made according to the percentage of matched behaviors, or according to whether the behavior signature 210 matched a specific subset of a known malware behavior signature.[7]

Thus, in view of the foregoing, the present application fully discloses, among other things:

- "wherein a plurality of different execution behaviors of the code module are recorded" and
- "to determine whether the plurality of different execution behaviors recorded in the behavior signature of the code module match a plurality of different execution behaviors recorded in a behavior signature of a known malware" and "the code module is a known malware based at least in part on the degree that the plurality of different execution behaviors recorded in the behavior signature of the code module match a plurality of different execution behaviors recorded in a behavior signature of the known malware."

Accordingly, this rejection under 35 U.S.C. 112, first paragraph should be withdrawn.

C. Response to Rejection under 35 U.S.C. 103(a)

Applicants traverse this rejection. As mentioned in Applicant's prior amendment, neither *White* nor *Schultz* discloses comparing a code module's plurality of different, executed behaviors with a plurality of different behaviors of a behavior signature of a particular known malware. Moreover, neither *White* nor *Schultz* discloses reporting whether that code module is the particular known malware based on that comparison.

As also mentioned in Applicant's prior amendment, *Schultz* merely uses a pattern matching of code segments to identify whether a program is malicious in general.[8] *Schultz* doesn't execute the program to identify behavior and certainly doesn't report that the program is a particular known malware based on such behavior. In fact, *Schultz* teaches away from executing the program: "All of the information about the binary is obtained from the program without executing the unknown program by examining the static properties of the binary...."[9]

As also mentioned in Applicant's prior amendment, *White* merely discloses a replication environment used to identify a single behavior: replication.[10] *White* doesn't use this fact (*i.e.*, the fact that a sample replicated itself) to determine that the sample is a particular virus. Instead, it

[7] *See* U.S. Patent Application Publication 2005/0188272 A1, [0035] (the present application) (emphasis added).
[8] *See Schultz*, ¶ [0043] (discussing a hexadecimal representation of the executable machine code).
[9] *See Schultz*, ¶ [0044] (emphasis added).
[10] *See* White, at 20-21.

merely determines that the sample is a virus and then generates a bit sequence signature string from the sample to be used to identify future viruses.[11] As discussed in background of the present application, hash sequences like this are inadequate because malware can be easily modified and thus the hash sequences of the modified malware do not match the hash sequences of the original, unmodified malware.

Despite the foregoing arguments, page 4 of the Office Action presents two arguments why two particular passages of *White* are relevant.

1. Response to First Argument Raised in Page 4 of the Office Action

Page 4 of the Office Action notes that "pages 13-15: paragraph 5, lines 1-2 and paragraph 6 scans the sample file against the latest virus definition." This passage does **not** disclose comparing a code module's plurality of different, executed behaviors with a plurality of different behaviors of a behavior signature of a particular known malware. This passage does **not** disclose reporting whether that code module is the particular known malware based on that comparison.

2. Response to Second Argument Raised in Page 4 of the Office Action

Page 4 of the Office Action quotes the following passage from *White*:

> The first step in analyzing a virus is to try to determine what type of virus it is, so that specialized type specific routines can be brought to bear. For Microsoft Word files, the classification task currently identifies the version of Word and determines, as best it can, the language of the file (English, French, etc.). For Microsoft Excel files, it determines the version of Excel. For DOS file viruses, it determines if they are COM or EXE files. To ensure reliability, this classification is done by examining the structure of the file, rather than by looking at the filetype.[12]

This passage does **not** disclose comparing a code module's plurality of different, executed behaviors with a plurality of different behaviors of a behavior signature of a particular known malware. This passage does **not** disclose reporting whether that code module is the particular known malware based on that comparison.

[11] *See* White, at 21 (discussing extracting "a good signature string").
[12] *White*, at 20.

D. Additional Features

Despite these traversals, Applicant has amended Independent claim 1 to recite additional features, in particular, "wherein the malware detection system is configured to report whether the code module is a known malware based at least in part on the degree that the plurality of different execution behaviors recorded in the behavior signature of the code module match **at least one of a plurality of different subsets of execution behaviors recorded in a behavior signature of the known malware, wherein the different subsets of execution behaviors are pre-specified for the known malware**. Applicant has amended independent claims 2-4 to recite similar features.

By way of overview, the present application discloses that malware may be identified using partial matches of execution behaviors.[13] For example, the present application discloses that multiple subsets may be specified for a malware:

> Alternatively, ***specific subsets of behaviors*** within known malware signatures ***may be specially identified***, such that if there is a positive match between behaviors in the behavior signature 210 and the subset of specially identified behaviors of a known malware behavior signature, the malware detection system 200 may report a more positive identification of malware. [14]

In contrast, systems such as those disclosed in U.S. Patent Application Publication 2002/0056076 A1 by Made and U.S. Patent Application Publication 2002/0035696 by Thacker do **not** provide for partial-match-based identification. Moreover, such systems do not provide pre-identification of subsets of execution behaviors recorded in a behavior signature for use in partial matching to identify a particular malware.

In view of the foregoing, Applicant respectfully submits that the other rejections to the claims are now moot and do not, therefore, need to be addressed individually at this time. It will be appreciated, however, that this should not be construed as Applicant acquiescing to any of the purported teachings or assertions made in the last action regarding the cited art or the pending application, including any official notice. Instead, Applicant reserves the right to challenge any of the purported teachings or assertions made in the last action at any appropriate time in the future, should the need arise. Furthermore, to the extent that the Examiner has relied on any

[13] *See* U.S. Patent Application Publication 2005/0188272 A1, ¶ [0027] (the present application) (discussing partial matches).
[14] *See* U.S. Patent Application Publication 2005/0188272 A1, ¶ [0027] (the present application) (emphasis added).

Official Notice, explicitly or implicitly, Applicant specifically requests that the Examiner provide references supporting the teachings officially noticed, as well as the required motivation or suggestion to combine the relied upon notice with the other art of record.

In the event that the Examiner finds remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney at (801) 533-9800.

The Commissioner is hereby authorized to charge payment of any of the following fees that may be applicable to this communication, or credit any overpayment, to Deposit Account No. 23-3178: (1) any filing fees required under 37 CFR § 1.16; and/or (2) any patent application and reexamination processing fees under 37 CFR § 1.17; and/or (3) any post issuance fees under 37 CFR § 1.20. In addition, if any additional extension of time is required, which has not otherwise been requested, please consider this a petition therefore and charge any additional fees that may be required to Deposit Account No. 23-3178.

Dated this 16th day of December, 2009.

Respectfully submitted,

RICK D. NYDEGGER
Registration No. 28,651
MICHAEL B. DODD
Registration No. 46,437
RYAN N. FARR
Registration No. 52,882
Attorneys for Applicant
Customer No. 47973

RDN:MBD:crb
2555853_1.DOC